PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H03K 3/84 — A1

(11) Internationale Veröffentlichungsnummer: **WO 00/54406**

(43) Internationales Veröffentlichungsdatum: 14. September 2000 (14.09.00)

(21) Internationales Aktenzeichen: PCT/EP00/01993

(22) Internationales Anmeldedatum: 8. März 2000 (08.03.00)

(30) Prioritätsdaten:
199 10 729.7 11. März 1999 (11.03.99) DE

(71)(72) Anmelder und Erfinder: VOGTS, Richard [DE/DE]; Engelbergerstrasse 1, D–79106 Freiburg (DE).

(74) Anwälte: SCHMITT, Hans usw.; Dreikönigstrasse 13, D–79102 Freiburg (DE).

(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: RANDOM SIGNAL GENERATOR AND METHOD FOR GENERATING A RANDOM SIGNALS

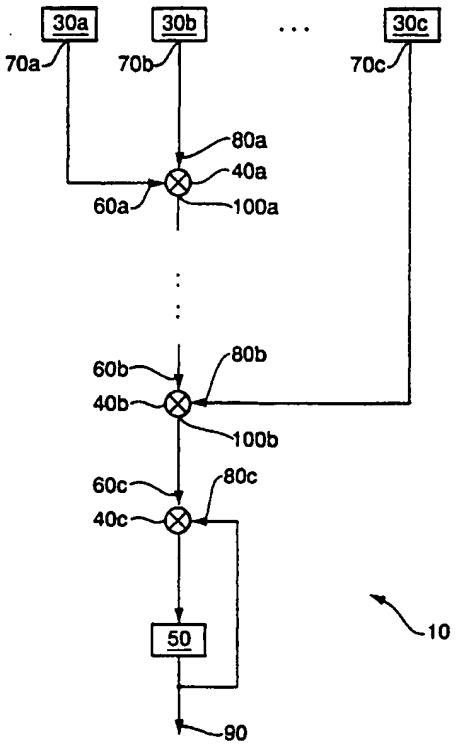
(54) Bezeichnung: ZUFALLSSIGNALGENERATOR SOWIE VERFAHREN ZUR ERZEUGUNG EINES ZUFALLSSIGNALS

(57) Abstract

The invention relates to a random signal generator (1) having at least two functional groups (2a, 2b, 2c) which each comprise a random sequence generator (3a, 3b, 3c), an exclusive–or gate (4a, 4b, 4c) and a memory element (5a, 5b, 5c). The exclusive–or gate (4a, 4b, 4c) of each functional group (2a, 2b, 2c) is in each case connected with one of its inputs (6a, 6b, 6c) to a random sequence signal output (7a, 7b, 7c) of the random sequence generator (3a, 3b, 3c) of the functional group (2a, 2b, 2c) and with its other input (8a, 8b, 8c) to a data output (9a, 9b, 9c) of the memory element (5a, 5b, 5c) of the functional group (2a, 2b, 2c). The output (10a, 10b, 10c) of the exclusive–or gate (4a, 4b, 4c) of each functional group (2a, 2b, 2c) is in each case connected to a data input (11a, 11b, 11c) of the memory element (5a, 5b, 5c) of the functional group (2a, 2b, 2c). The memory elements (5a, 5b, 5c) of the functional groups (2a, 2b, 2c) are interconnected via data lines (13) for the shifting of their memory contents.

(57) Zusammenfassung

Ein Zufallssignalgenerator (1) hat wenigstens zwei Funktionsgruppen (2a, 2b, 2c), die jeweils einen Zufallsfolgengenerator (3a, 3b, 3c), ein Exklusiv–Oder–Gatter (4a, 4b, 4c) und ein Speicherelement (5a, 5b, 5c) aufweisen. Das Exklusiv–Oder–Gatter (4a, 4b, 4c) jeder Funktionsgruppe (2a, 2b, 2c) ist jeweils mit einem seiner beiden Eingänge (6a, 6b, 6c) mit einem Zufallsfolgensignal–Ausgang (7a, 7b, 7c) des Zufallsfolgengenerators (3a, 3b, 3c) der Funktionsgruppe (2a, 2b, 2c) und mit seinem anderen Eingang (8a, 8b, 8c) mit einem Datenausgang (9a, 9b, 9c) des Speicherelements (5a, 5b, 5c) der Funktionsgruppe (2a, 2b, 2c) verbunden. Der Ausgang (10a, 10b, 10c) des Exklusiv–Oder–Gatters (4a, 4b, 4c) jeder Funktionsgruppe (2a, 2b, 2c) ist jeweils mit dem Dateneingang (11a, 11b, 11c) des Speicherelements (5a, 5b, 5c) der Funktionsgruppe (2a, 2b, 2c) verbunden. Die Speicherelemente (5a, 5b, 5c) der Funktionsgruppen (2a, 2b, 2c) sind zum Verschieben ihrer Speicherinhalte über Datenleitungen (13) miteinander verbunden.



Zufallssignalgenerator sowie Verfahren zur Erzeugung eines Zufallssignals

Die Erfindung betrifft ein Verfahren zur Erzeugung eines Zufallssignals und einen Zufallssignalgenerator.

Aus WO 97/43709 kennt man bereits einen Zufallssignalgenerator, der einen nichtdeterministischen Zufallsfolgengenerator aufweist, der einen spannungsgesteuerten Oszillator hat, dessen Frequenzsteuereingang mit einer Rauschspannungsquelle verbunden ist. Der Oszillator weist an seinem Ausgang ein Oszillatorsignal auf, dessen Frequenz entsprechend der an dem Frequenzsteuereingang anliegenden, sich stochastisch ändernden Rauschspannung zufällig um eine Mittenfrequenz schwankt. Der Zufallsfolgengenerator hat mehrere dynamische Flip-Flops, die jeweils mit ihrem Dateneingang an einem ihnen zugeordneten Ring-Oszillator angeschlossen sind. Dabei ist für jedes Flip-Flop jeweils ein eigener Ring-Oszillator vorgesehen, wobei die Frequenzen dieser Ring-Oszillatoren etwas voneinander abweichen und jeweils größer sind als die Frequenz des spannungsgesteuerten Oszillators des Zufallsignalgenerators. Die Takteingänge der Flip-Flops sind jeweils mit dem Ausgang des Zufallsignalgenerators verbunden, so daß bei einer Taktflanke des sich zufällig in der Frequenz verändernden Schwingungssignales des spannungsgesteuerten Oszillators jeweils ein Signalwert der einzelnen Schwingungssignale der Ring-Oszillatoren abgetastet und in das dem betreffenden Ring-Oszillator zugeordnete Flip-Flop eingelesen wird. Die in den einzelnen Flip-Flops zwischengespeicherten Signalwerte werden dann jeweils an einem Ausgang der Flip-Flops ausgegeben und bilden das zu erzeugende Zufallssignal. Dabei representieren die an den Ausgängen der Flip-Flops anliegenden Signale jeweils eine Binärziffer einer zu erzeugenden, mehrere Ziffern aufweisenden Zufallszahl. Nach Angabe der Patentschrift sollen die Binärwerte der am Ausgang der Flip-Flops anliegenden Ziffernsignale gleich verteilt sein, d.h. heißt die

BESTÄTIGUNGSKOPIE

Ausgänge der Flip-Flops sollen jeweils im Mittel ein etwa gleich großen Anzahl logischer "Einsen" und "Nullen" liefern.

Der vorbekannte Zufallszahlengenerator hat jedoch den Nachteil, daß die einzelnen Ziffernsignale beziehungsweise die diesem zugeordneten Binärstellen der Zufallszahl noch eine gewisse Abhängigkeit voneinander aufweisen. Auch kann es zu einer Korrelation von zwei Zufallszahlen kommen, die unmittelbar nacheinander aus dem Zufallssignalgenerator ausgelesen werden. Ein Beobachter kann deshalb durch entsprechend langes Beobachten der von dem Zufallszahlengenerator ausgegebenen Zufallszahlen auf die Eigenschaften des Zufallssignal- oder Zufallszahlengenerators, insbesondere auf die Eigenschaften der darin enthaltenen Ringoszillatoren schließen. Ungünstig ist außerdem, daß ein Defekt in der Rauschspannungsquelle und/oder dem spannungsgesteuerten Oszillator des Zufallsignalgenerators zur Folge haben kann, daß der spannungsgesteuerte Oszillator mit einer konstanten Frequenz schwingt, so daß die Korrelation der Zufallszahlen dann stark zunimmt, d.h. die Zufälligkeit des Zufallssignals bzw. der durch dieses Signal repräsentierten Zufallszahlen nimmt ab, ohne daß dies der Benutzer des Zufallszahlengenerators bemerkt. Für bestimmte Anwendungen, wie beispielsweise bei der Verschlüsselung von Nachrichten oder der Identifikation eines Absenders einer Nachricht mittels einer "digitalen" Unterschrift, ist es jedoch erforderlich, daß die Zufälligkeit des erzeugten Zufallssignales bzw. der Zufallszahlen möglichst groß ist und somit die Zufallszahlen praktisch nicht vorhersagbar sind.

Aus EP 0 782 069 A1 kennt man auch bereits einen Pseudo-Zufallszahlengenerator, der mehrere deterministische Zufallsfolgengeneratoren aufweist, die jeweils einen Ausgang für ein Pseudo-Zufallssignal haben. Diese Ausgänge sind jeweils mit einem Eingang einer Kombinationseinrichtung verbunden, die einen Ausgang für ein durch nichtlineare Kombination der Pseudo-Zufallssignale

gebildetes Kombinationssignal aufweist. Der Kombinationssignal-Ausgang ist mit dem Dateneingang eines mehrere Speicherelemente aufweisenden Schieberegisters verbunden, in das die aus dem Kombinationssignal-Ausgang ausgelesenen Daten sequentiell einlesbar sind. Die Datenausgänge der Speicherelemente des Schieberegisters sind jeweils mit einem Eingang einer nichtlinearen Verknüpfungseinrichtung verbunden. Diese weist einen Ausgang für ein Signal auf, das durch nichtlineare Kombination der an den Datenausgängen der Speicherelemente des Schieberegisters anliegenden Datensignale gebildet ist. An diesem Ausgang werden die einzelnen Stellen der zu erzeugenden Zufallszahl nacheinander synchron zu einem Taktsignal ausgegeben. Der vorbekannte Pseudo-Zufallszahlengenerator hat den Nachteil, daß das an dem Ausgang der Verknüpfungseinrichtung anliegende Signal trotz der vergleichsweise aufwendigen Kombination mehrerer Pseudo-Zufallssignale zu einem Zufallszahlensignal durch eine mathematische Funktion beschreibbar ist. Die mit dem Zufallszahlengenerator erzeugten Zufallszahlen sind deshalb bei Kenntnis dieser mathematischen Funktion und des Zustands des Zufallssignalgenerators vorhersagbar. Ungünstig ist außerdem, daß der Zufallssignalgenerator noch einen vergleichsweise komplizierten Aufbau aufweist.

Man kennt auch bereits einen Zufallssignalgenerator, bei dem ein analoges Rauschsignal einer Rauschquelle mit einem Hochfrequenzverstärker verstärkt und der Signalpegel dieses Verstärkers anschließend digitalisiert wird. Am Ausgang des Hochfrequenzverstärkers wird dann die zu erzeugende Zufallszahl sequentiell ausgelesen, wobei die beiden durch die Digitalisierung des Verstärker-Ausgangssignals definierten Signalpegel als Binärwerte einer Binärzahl interpretiert werden. Dieser Zufallssignalgenerator ist jedoch ebenfalls relativ teuer, da zur Vermeidung von Korrelationen zwischen dem digitalen Ausgangssignal des Zufallssignalgenerators und dem analogen

Rauschsignal eine aufwendige Abschirmung des Hochfrequenzverstärkers erforderlich ist. Außerdem muß die Rauschquelle gegen äußere elektromagnetische Störungen abgeschirmt sein.

Es besteht deshalb die Aufgabe, ein Verfahren zur Erzeugung eines Zufallssignals anzugeben, das statistisch weitgehend voneinander unabhängige und gleichverteilte Signalpegel oder Zufallswerte aufweist. Außerdem besteht die Aufgabe, einen Zufallssignalgenerator zu schaffen, der einfach aufgebaut ist, mit dem aber dennoch statistisch weitgehend voneinander unabhängige und gleichverteilte Signalpegel, Zufallswerte oder Zufallszahlen erzeugt werden können.

Die Lösung dieser Aufgabe besteht bezüglich des Verfahrens darin, daß mittels wenigstens zweier nichtdeterministischer Zufallsfolgengeneratoren zumindest zwei Zufallsfolgensignale erzeugt und exklusiv-oder-verknüpft werden und daß das Exklusiv-Oder-Ausgangssignal das Zufallssignal oder ein Zwischensignal zur Weiterverarbeitung bildet.

In vorteilhafter Weise wird dadurch ein Zufallssignal bereitgestellt, das eine größere Zufälligkeit aufweist, als die einzelnen Zufallsfolgensignale, aus denen das Zufallssignal gemischt wurde. Somit kann eine gute Annäherung der statistischen Verteilung der Signalpegel oder Zufallswerte des generierten Zufallssignal an eine Gleichverteilung erreicht werden.

Bei einer Ausführungsform des Verfahrens ist vorgesehen, daß das Exklusiv-Oder-Ausgangssignal als Zwischensignal mit dem Zufallsfolgensignal wenigstens eines weiteren nichtdeterministischen Zufallsfolgengenerators exklusiv-oder-verknüpft wird und das Exklusiv-Oder-Ausgangssignal dieser Verknüpfung das Zufallssignal oder ein Zwischensignal zur Weiterverarbeitung bildet. Die statistische Verteilung der Signalpegel oder

Zufallswerte des generierten Zufallssignals ist dann noch besser an eine Gleichverteilung angenähert.

Besonders vorteilhaft ist, wenn aus dem Zwischensignal ein Zufallssignalwert ermittelt wird, indem einem Exklusiv-Oder-Glied dieses Zwischensignals sowie ein zwischengespeichertes Ausgangssignal des Exklusiv-Oder-Gliedes zugeführt wird. Es werden also zu unterschiedlichen Zeitpunkten generierte Zufallsfolgensignalwerte miteinander exklusiv-oder-verknüpft, wodurch eine noch größere Zufälligkeit der Signalpegel oder Zufallswerte des generierten Zufallssignals erreicht wird.

Die vorstehend genannte Aufgabe kann bezüglich des Verfahrens auch dadurch gelöst werden, daß mittels wenigstens zweier nichtdeterministischer Zufallsfolgengeneratoren wenigstens zwei Zufallsfolgensignale erzeugt werden,

a) daß jeweils ein Zufallssignalwert aus jedem der Zufallsfolgensignale der einzelnen Zufallsfolgengeneratoren ermittelt wird und mit einem einem anderen Zufallsfolgengenerator zugeordneten Speicherwert exklusiv-oder-verknüpft wird,

b) das Ergebnis dieser Verknüpfung jeweils als neuer, dem zuerstgenannten Zufallsfolgengenerator zugeordneten Speicherwert zwischengespeichert wird,

c) daß die Verfahrensschritte a) und b) als Schleife wenigstens einmal erneut durchlaufen werden

d) und daß danach die den einzelnen Zufallsfolgengeneratoren jeweils zugeordneten Speicherwerte als Zufallssignal ausgegeben werden.

Es werden also mehrere Zufallsfolgensignale mit Hilfe von unterschiedlichen Zufallsfolgengeneratoren erzeugt, wobei diese Zufallsfolgensignale mittels Exklusiv-oder-Verknüpfungen entsprechend den Verfahrensschritten a) bis d) miteinander

kombiniert werden. In vorteilhafter Weise kann dadurch ein Zufallssignal bereitgestellt werden, das eine größere Zufälligkeit aufweist, als die einzelnen Zufallsfolgensignale, aus denen das Zufallssignal gemischt wurde. Das Verfahren ermöglicht es deshalb, mittels mehrerer vergleichsweise einfach aufgebauter Zufallssignalgeneratoren Zufallszahlen oder Zufallssignale zu ermitteln, die praktisch nicht miteinander korreliert sind und deren Häufigkeit nahezu gleich verteilt ist.

Vorteilhaft ist, wenn die Verfahrensschritte a) bis d) mehrmals durchlaufen werden. Dadurch ist es möglich, Zufallszahlen zu erzeugen, die eine größere Anzahl Ziffern oder Stellen aufweisen als die Anzahl der Zufallssignalgeneratoren.

Vorteilhaft ist, wenn die Speicherwerte in einem Datenspeicher zyklisch verschoben werden. Die mittels der einzelnen Zufallsfolgengeneratoren generierten Zufallssignalwerte können dann noch besser gemischt werden.

Besonders vorteilhaft ist, wenn die Zufallsfolgengeneratoren jeweils vor dem erneuten Abarbeiten des Verfahrensschritt a) in einen definierten Zustand zurückgesetzt werden. Dadurch kann die Korrelation zweier unmittelbar nacheinander ermittelter Signalwerte des Zufallssignals zusätzlich reduziert werden.

Eine bevorzugte Ausführungsform des Verfahrens sieht vor, daß zum Erzeugen der Zufallsfolgensignale der Zufallsfolgengeneratoren jeweils die Frequenz eines spannungsgesteuerten Oszillators mittels eines Rauschspannungssignals verändert wird und daß der Zufallssignalwert jeweils aus dem Oszillatorsignal des Oszillators ermittelt wird. Die Zufallssignale können dadurch auf einfache Weise bereits mit einer vergleichsweise guten Gleichverteilung ihrer Zufallssignalwerte erzeugt werden.

Besonders vorteilhaft ist, wenn jeweils vor dem erneuten Abarbeiten des Verfahrensschritts a) eine definierte Zeitdauer, die gleich oder größer als die Periodendauer des Oszillatorsignals ist, abgewartet wird. Die Wartezeit kann beispielsweise größer als das zehnfache der Periodendauer sein. Nacheinander bzw. aufeinanderfolgend aus dem Zufallssignal ermittelte Zufallssignalwerte oder Zufallszahlen weisen dann untereinander eine noch geringere Korrelation auf.

Die Lösung der vorstehend genannten Aufgabe besteht bezüglich des Zufallssignalgenerators darin, daß der Zufallssignalgenerator wenigstens zwei nichtdeterministische Zufallsfolgengeneratoren und zumindest ein Exklusiv-Oder-Gatter aufweist, daß die Eingänge des Exklusiv-Oder-Gatters mit Zufallsfolgensignale liefernden Zufallsfolgengeneratoren verbunden sind, und daß der Ausgang des Exklusiv-Oder-Gatters direkt oder indirekt über eine Zwischenstufe zur Weiterverarbeitung des Exklusiv-Oder-Gatter-Ausgangssignales mit einem Zufallssignal-Ausgang des Zufallssignalgenerators verbunden ist.

In vorteilhafter Weise weist das von dem Zufallssignalgenerator erzeugte Zufallssignal eine größere Zufälligkeit auf, als die einzelnen Zufallsfolgensignale, aus denen das Zufallssignal gemischt wurde. Somit kann auch bei Verwendung einfach aufgebauter Zufallsfolgengeneratoren eine gute Annäherung der statistischen Verteilung der Signalpegel oder Zufallswerte des generierten Zufallssignal an eine Gleichverteilung erreicht werden.

Vorteilhaft ist, wenn die Zwischenstufe ein Exklusiv-Oder-Gatter aufweist, dessen einer Eingang mit dem Ausgang des mit den Zufallsfolgengeneratoren verbundenen Exklusiv-Oder-Gatter und dessen anderer Eingang mit dem Zufallsfolgensignal-Ausgang eines weiteren Zufallsfolgengenerators verbunden ist, und wenn der Ausgang dieses Exklusiv-Oder-Gatters direkt oder indirekt über

eine Zwischenstufe zur Weiterverarbeitung des Exklusiv-Oder-Gatter-Ausgangssignales mit dem Zufallssignal-Ausgang des Zufallssignalgenerators verbunden ist. Die statistische Verteilung der Signalpegel oder Zufallswerte des mittels des Zufallssignalgenerators erzeugten Zufallssignals ist dann noch besser an eine Gleichverteilung angenähert.

Bei einer zweckmäßigen Ausgestaltung der Erfindung ist vorgesehen, daß die Zwischenstufe ein Exklusiv-Oder-Gatter aufweist, dessen einer Eingang direkt oder indirekt über eine weitere Zwischenstufe mit dem Ausgang des mit den Zufallsfolgengeneratoren verbundenen Exklusiv-Oder-Gatter verbunden ist, und daß an den Ausgang des zuerstgenannten Exklusiv-Oder-Gatters ein Speicherelement angeschlossen ist, dessen Ausgang über eine Rückkoppelschleife mit dem zweiten Eingang dieses Exklusiv-Oder-Gatters verbunden ist. Dadurch ist es möglich, zu unterschiedlichen Zeitpunkten generierte Zufallsfolgensignalwerte miteinander exklusiv-oder zu verknüpfen, wodurch eine noch größere Zufälligkeit der Signalpegel oder Zufallswerte des generierten Zufallssignals erreicht wird.

Die vorstehend genannte Aufgabe kann bezüglich des Zufallssignalgenerators auch dadurch gelöst werden, daß der Zufallssignalgenerator wenigstens zwei Funktionsgruppen hat, die jeweils einen nichtdeterministischen Zufallsfolgengenerator, ein Exklusiv-Oder-Gatter und ein Speicherelement aufweisen, wobei das Exklusiv-Oder-Gatter jeder Funktionsgruppe jeweils mit einem seiner beiden Eingänge mit einem Zufallsfolgensignal-Ausgang des Zufallsfolgengenerators der Funktionsgruppe und mit seinem anderen Eingang mit einem Datenausgang des Speicherelements der Funktionsgruppe verbunden ist, wobei der Ausgang des Exklusiv-Oder-Gatters jeder Funktionsgruppe jeweils mit dem Dateneingang des Speicherelements der Funktionsgruppe verbunden ist, und wobei die Speicherelemente der Funktionsgruppen zum Verschieben ihrer

Speicherinhalte über Datenleitungen miteinander verbunden sind.

In vorteilhafter Weise werden also jeweils die Signalwerte des zu erzeugenden Zufallssignales aus den Zufallssignalwerten mehrerer, vorzugsweise aller Zufallsfolgengeneratoren gebildet, wodurch die Signalwerte des Zufallssignales eine größere Zufälligkeit aufweisen als die aus den Zufallsfolgensignalen der Zufallsfolgengeneratoren ermittelten Zufallssignalwerte. Der Zufallssignalgenerator ermöglicht deshalb die Ermittlung von Zufallssignalen mit nahezu perfekt gleich verteilter Häufigkeit ihrer Signalwerte, selbst dann, wenn die Häufigkeit der Zufallsfolgensignalwerte der einzelnen Zufallsfolgengeneratoren - wie dies in der Praxis immer der Fall ist - von der idealen Gleichverteilung abweicht. Außerdem weisen nacheinander mit dem Zufallssignalgenerator ermittelte Zufallssignalwerte nur eine sehr geringe Korrelation auf. Die einzelnen Zufallsfolgengeneratoren des Zufallssignalgenerators können deshalb einen vergleichsweise einfachen Aufbau aufweisen, wodurch sich insgesamt ein einfach aufgebauter und kostengünstig herstellbarer Zufallssignalgenerator ergibt. In vorteilhafter Weise kann bei einem Zufallssignalgenerator, der mehr als zwei Zufallsfolgengeneratoren aufweist, selbst dann noch eine gute Gleichverteilung der Häufigkeit der Zufallssignalwerte und eine geringe Korrelation zwischen den einzelnen Zufallssignalwerten erreicht werden, wenn einer der Zufallsfolgengeneratoren einmal ausfallen sollte oder wenn aus anderen Gründen, beispielsweise durch Umgebungseinflüsse (Temperatur, elektromagnetische Felder, Manipulationsversuche usw.) und/oder Alterungsprozesse, ein Verlust der Zufälligkeit der Zufallsfolgensignalwerte auftreten sollte. Der Zufallssignalgenerator weist deshalb eine hohe Betriebssicherheit auf.

Die vorstehend genannte Aufgabe kann bezüglich des Zufallssignalgenerators auch dadurch gelöst werden, daß der Zufallssignalgenerator wenigstens zwei Funktionsgruppen hat, die jeweils

einen Zufallsfolgengenerator, ein Exklusiv-Oder-Gatter und ein Speicherelement aufweisen, wobei das Exklusiv-Oder-Gatter jeder Funktionsgruppe jeweils mit einem seiner beiden Eingänge mit einem Zufallsfolgensignal-Ausgang des Zufallsfolgengenerators der Funktionsgruppe und mit seinem anderen Eingang mit einem Datenausgang des Speicherelements einer anderen Funktionsgruppe verbunden ist, und wobei der Ausgang des Exklusiv-Oder-Gatters jeweils mit dem Dateneingang des Speicherelements der zuerst genannten Funktionsgruppe verbunden ist.

Zusätzlich zu den Vorteilen der Lösung gemäß Anspruch 14 hat diese Lösung noch den Vorteil, daß zusätzliche Datenleitungen zum Verschieben der Speicherinhalte zwischen den Speicherelementen entfallen können.

Eine Ausführungsform der Erfindung sieht vor, daß das Speicherelement oder die Speicherelemente Teil eines Ringschieberegister sind. Die Speicherinhalte der Speicherelemente können dann auf einfache Weise nach jeder Exklusiv-Oder-Verknüpfung der Zufallssignalwerte mit den Speicherinhalten in dem Ringspeicher zyklisch verschoben werden. Dabei ist es sogar möglich, daß das Ringschieberegister zusätzlich zu den Speicherelementen der Funktionsgruppen Zwischenspeicherelemente aufweist. In den Zwischenspeicherelementen können dann zusätzliche Ziffern einer zu ermittelnden Zufallszahl zwischengespeichert werden. Die Ziffern- oder Stellenzahl der einzelnen Zufallszahlen kann dann größer sein als die Anzahl der Zufallsfolgengeneratoren des Zufallssignalengenerators.

Besonders vorteilhaft ist, wenn die Zufallssignalgeneratoren einen Rücksetzeingang aufweisen, mittels dem die Zufallssignale der Zufallsfolgengeneratoren in einen definierten Zustand überführbar sind. Die Zufallsfolgengeneratoren können dann vor dem Ermitteln einer neuen Zufallszahl jeweils in einen definierten

Ausgangszustand gebracht werden, wodurch die Korrelation zwischen aufeinanderfolgend ermittelten Zufallszahlen vermindert wird.

Bei einer bevorzugten Ausführungsform der Erfindung weisen die Zufallsfolgengeneratoren jeweils einen spannungsgesteuerten Oszillator auf, dessen Frequenzsteuereingang mit einer Rauschspannungsquelle verbunden ist, wobei der Oszillator-Ausgang mit dem Zufallsfolgensignalausgang des Zufallsfolgengenerators verbunden ist. Die Zufallsfolgensignale können dadurch auf einfache Weise und mit einer vergleichsweise guten Gleichverteilung der Häufigkeit ihrer Zufallsfolgensignalwerte erzeugt werden.

Vorteilhaft ist, wenn der Oszillator-Ausgang mit dem Eingang eines Flip-Flops oder dergleichen Frequenzteiler verbunden ist und wenn der Ausgang des Flip-Flop mit dem Zufallsfolgensignalausgang des Zufallsfolgengenerators verbunden ist. Das Flip-Flop invertiert dann mit jedem Taktimpuls des Oszillators sein Ausgangssignal, wodurch eine bessere Gleichverteilung der aus den am Ausgang des Zufallssignalgenerators anliegenden Zufallssignals ermittelten Zufallssignalwerten erreicht wird.

Besonders vorteilhaft ist, wenn zumindest das oder die Exklusiv-Oder-Gatter und gegebenenfalls das Ringschieberegister Teil eines Mikroprozessors sind. Der Zufallssignalgenerator ist dann besonders kostengünstig herstellbar und kann beispielsweise als Einsteckkarte ausgebildet sein, die einen Bus-Anschluß zum Verbinden mit dem Systembus eines Mikrocomputers aufweist.

Nachfolgend sind Ausführungsbeispiele der Erfindung anhand der Zeichnung näher erläutert. Es zeigen:

Fig. 1, 2 ein Schaltbild eines Zufallssignalgenerators, der mehrere Zufallsfolgengeneratoren aufweist, von denen

jedoch nur drei dargestellt sind,

Fig. 3, 5 ein Schaltbild eines Zufallssignalgenerators, der mehrere Funktionsgruppen sowie mehrere Zwischenspeicherelemente aufweist, wobei von den Funktionsgruppen nur drei und von den Zwischenspeicherelementen nur eines dargestellt ist,

Fig. 4 eine Abwandlung des Schaltbilds nach Figur 3, wobei der Zufallssignalgenerator anstelle des in Fig. 3 gezeigten parallelen Zufallssignalausgangs einen seriellen Zufallssignalausgang hat,

Fig. 6 eine Abwandlung des Schaltbilds nach Figur 5, wobei der Zufallssignalgenerator anstelle des in Fig. 5 gezeigten parallelen Zufallssignalausgangs einen seriellen Zufallssignalausgang hat, und

Fig. 7 ein Blockschaltbild des Zufallssignalgenerators.

Der in Fig. 1 gezeigte, im ganzen mit 10 bezeichnete Zufallssignalgenerator weist mehrere nichtdeterministische Zufallsfolgengeneratoren 30a, 30b, 30c und mehrere Exklusiv-Oder-Gatter 40a, 40b, 40c auf. Der Zufallsfolgensignalausgang 70a des Zufallsfolgengenerators 30a ist mit einem ersten Eingang 60a und der Zufallsfolgensignalausgang 70b des Zufallsfolgengenerators 30b ist mit einem zweiten Eingang 60a des Exklusiv-Oder-Gatter 40a verbunden. Das am Ausgang 100a des Exklusiv-Oder-Gatters 40a anliegende, durch Mischung der Zufallsfolgensignale der beiden Zufallsfolgengeneratoren 30a, 30b gebildete Zwischensignal weist eine größeren Zufallsgehalt auf als jedes der beiden an den Eingängen 60a, 80a anliegende Zufallsfolgensignale.

Das am Ausgang 100a des Exklusiv-Oder-Gatters 40a anliegende

Zwischensignal ist direkt oder indirekt über wenigstens eine, in der Zeichnung nicht dargestellte Zwischenstufe zur Weiterverarbeitung des Zwischensignales mit dem ersten Eingang 60b des Exklusiv-Oder-Gatters 40b verbunden. Der zweite Eingang 80b dieses Exklusiv-Oder-Gatters 40b ist an dem Zufallsfolgensignalausgang 70c eines weiteren Zufallsfolgengenerators 30b angeschlossen. Das an dem mit einem Ausgangsanschluß des Zufallssignalgenerators 10 verbundenen Ausgang 100b des Exklusiv-Oder-Gatters 40b anliegende Zufallssignal weist einen größeren Zufallsgehalt auf als jedes der Zufallsfolgensignalausgänge 70a, 70b, 70c. Somit ergibt sich eine gute Annäherung der Verteilung der Signalwerte des Zufallssignales an eine Gleichverteilung.

Zwischen dem Ausgang 100a des Exklusiv-Oder-Gatters 40a und dem Eingang 60b des Exklusiv-Oder-Gatters 40b kann wenigstens eine Zwischenstufe angeordnet sein oder es können mehrere in Reihe geschaltete Zwischenstufen vorgesehen sein. Diese Zwischenstufen entsprechen jeweils in ihrem Aufbau der aus dem Exklusiv-Oder-Gatters 40b und dem Zufallsfolgengenerator 30c gebildeten Anordnung, wobei jeweils ein Eingang des Exklusiv-Oder-Gatters der Zwischenstufe mit dem Ausgang des in der Reihe benachbart vorgeschalteten Exklusiv-Oder-Gatters und der Ausgang des Exklusiv-Oder-Gatters der Zwischenstufe mit einem Eingang des in der Reihe benachbart nachgeschalteten Exklusiv-Oder-Gatters verbunden ist.

Wie in Figur 2 erkennbar ist, kann dem Exklusiv-Oder-Gatter 40b eine Zwischenstufe nachgeschaltet sein, die ein weiteres Exklusiv-Oder-Gatter 40c aufweist, dessen erster Eingang 60c mit dem Ausgang 100b des Exklusiv-Oder-Gatters 40b verbunden ist. An den Ausgang des Exklusiv-Oder-Gatters 40c ist der Dateneingang eines Speicherelements 50 angeschlossen ist, dessen Ausgang über eine Rückkoppelschleife mit dem zweiten Eingang 80c dieses

Exklusiv-Oder-Gatters 40c verbunden ist. Durch diese Maßnahme wird erreicht, daß zeitlich nacheinader von den Zufallsfolgengeneratoren 30a, 30b, 30c generierte Zufallsfolgenwerte bzw. daraus abgeleitete Signale miteinander gemischt werden. Der Datenausgang des Speicherelements 50 ist mit dem Zufallssignalausgang des Zufallssignalgenerators 10 verbunden.

Die in Fig. 3 bis 6 gezeigten, im ganzen mit 1 bezeichneten Zufallssignalgeneratoren haben jeweils mehrere Funktionsgruppen 2a, 2b, 2c, die jeweils einen nichtdeterministischen Zufallsfolgengenerator 3a, 3b, 3c, ein Exklusiv-Oder-Gatter 4a, 4b, 4c und ein Speicherelement 5a, 5b, 5c aufweisen. Bei dem Ausführungsbeispiel nach Fig. 3 ist das Exklusiv-Oder-Gatter 4a, 4b, 4c jeder Funktionsgruppe 2a, 2b, 2c jeweils mit einem seiner beiden Eingänge 6a, 6b, 6c mit einem Zufallssignal-Ausgang 7a, 7b, 7c des Zufallsfolgengenerators 3a, 3b, 3c der Funktionsgruppe 2a, 2b, 2c und mit seinem anderen Eingang 8a, 8b, 8c mit einem Datenausgang 9a, 9b, 9c des Speicherelements 5a, 5b, 5c der Funktionsgruppe 2a, 2b, 2c verbunden. In Fig. 3 ist ferner erkennbar, daß die Speicherelemente 5a, 5b, 5c Teil eines Ringschieberegisters sind und daß dieses zusätzlich noch Zwischenspeicherelemente 12 aufweist, die mit den Speicherelementen 5a, 5b, 5c der Funktionsgruppen 2a, 2b, 2c mittels Datenleitungen 13 zu einem Ring verschaltet sind. Mittels der Datenleitungen 13 sind die in den Speicherelementen 5a, 5b, 5c abgelegten Speicherwerte zyklisch in dem Ringschieberegister verschiebbar.

Nachfolgend sind die einzelnen Verarbeitungsschritte des Zufallssignalgenerators 1 bei der Ermittlung eines Zufallssignals bzw. einer Zufallszahl näher erläutert. Zunächst werden die Speicherelemente 5a, 5b, 5c und die Zwischenspeicher 12 jeweils mit einem vorgegebenen Speicherwert vorbesetzt, beispielsweise einer logischen 0 oder einer logischen 1. Aus dem

Zufallssignal jedes der Zufallsfolgengeneratoren 3a, 3b, 3c wird jeweils ein Zufallsfolgensignalwert ermittelt, beispielsweise durch Abtasten des Zufallsfolgensignals. Das diesem Zufallsfolgensignalwert entsprechende, jeweils an dem Zufallssignalausgang 7a, 7b, 7c einer Funktionsgruppe 2a, 2b, 2c anliegende Signal wird jeweils mit dem in dem Speicherelement 5a, 5b, 5c der Funktionsgruppe 2a, 2b, 2c abgelegten Speicherwert entsprechenden, an dem Datenausgang 9a, 9b, 9c anliegenden Datensignal in dem Gatter 4a, 4b, 4c Exklusiv-Oder-Verknüpft. Das Ergebnis dieser Verknüpfung wird mittels des Dateneingangs 11a, 11b, 11c jeweils als neuer Speicherwert in das jeweilige Speicherelement 5a, 5b, 5c der betreffenden Funktionsgruppe 2a, 2b, 2c eingespeichert.

Danach werden die Speicherwerte in dem durch die Speicherelemente 5a, 5b, 5c und die Zwischenspeicherelemente 12 gebildeten Ringspeicher um eine der Anzahl der Zufallsfolgengeneratoren 3a, 3b, 3c entsprechende Anzahl Stellen oder Bit in dem Ringspeicher nach rechts verschoben. Da die Anzahl der Speicherelemente 5a, 5b, 5c der Anzahl der Zwischenspeicherelemente 12 entspricht, sind die zuvor in den Speicherelementen 5a, 5b, 5c abgelegten Signalwerte nun in den Zwischenspeicherelementen zwischengespeichert.

Danach werden die Zufallsfolgensignale der Zufallsfolgengeneratoren 3a, 3b, 3c jeweils in den Ausgangszustand zurückversetzt. Anschließend wird eine definierte Zeit abgewartet, bis die Zufallsfolgensignale der Zufallsfolgengeneratoren 3a, 3b, 3c jeweils einen zufälligen Wert angenommen haben. Aus den einzelnen Zufallsfolgensignalen der Funktionsgruppen 2a, 2b, 2c wird dann jeweils ein Zufallsfolgensignalwert ermittelt. Dieser wird in der zuvor beschriebenen Weise mittels des Exklusiv-Oder-Gatters 4a, 4b, 4c der jeweiligen Funktionsgruppe 2a, 2b, 2c mit dem in dem Speicherelement 5a, 5b, 5c dieser Funktionsgruppe 2a,

2b, 2c enthaltenen Speicherwert Exklusiv-Oder-Verknüpft und in dem jeweiligen Speicherelement 5a, 5b, 5c der Funktionsgruppe 2a, 2b, 2c abgelegt.

Danach werden die in dem Ringschieberegister gespeicherten Datenwerte um eine Anzahl Stellen, die um 1 größer ist als die Anzahl der Zufallsfolgengeneratoren 3a, 3b, 3c in dem Ringschieberegister zyklisch nach rechts verschoben. Außerdem werden die Zufallsfolgensignale der Zufallsfolgengeneratoren 3a, 3b, 3c in den Ausgangszustand zurückgesetzt. Danach wird eine definierte Zeit abgewartet, bis die Zufallsfolgensignale jeweils einen zufälligen Wert angenommen haben.

Die vorstehend beschriebenen Verarbeitungsschritte können mit Ausnahme des ersten Verarbeitungsschritts, bei dem die Speicherelemente 5a, 5b, 5c und die Zwischenspeicher 12 vorbesetzt werden, als Schleife gegebenenfalls noch ein oder mehrmals wiederholt werden. In der Praxis hat es sich als vorteilhaft erwiesen, wenn bei einem Zufallssignalgenerator 1, dessen Ringschieberegister eine Breite von 8 Bit aufweist, die durch die genannten Verarbeitungsschritte definierte Schleife insgesamt 16 mal durchlaufen wird, d.h. es werden 16 vollständige Primärbytes eingelesen und verarbeitet. Danach wird die Zufallszahl an den Datenausgängen 9a, 9b, 9c, 9d parallel als Binärzahl ausgelesen.

Die mittels des Zufallssignalgenerators 1 erzeugten Zufallszahlen weisen bezüglich ihrer Häufigkeit nahezu eine Gleichverteilung auf. Dabei sind die einzelnen Zufallszahlen nicht oder nicht nennenswert korreliert. Dies wird vor allem dadurch erreicht, daß die mittels der unterschiedlichen Zufallsfolgengeneratoren 3a, 3b, 3c erzeugten Zufallssignalwerte miteinander vermischt werden. Die Zufallssignalwerte sind untereinander unkorreliert. Bei der Verknüpfung der jeweils an den Eingängen 6a, 6b, 6c und

8a, 8b, 8c der Exklusiv-Oder-Gatter 4a, 4b, 4c anliegenden, einen bestimmten Zufallsgehalt aufweisenden Eingangssignale ergibt sich deshalb an den Ausgängen 10a, 10b, 10c der Exklusiv-Oder-Gatter 4a, 4b, 4c ein Ausgangssignal, das einen größeren Zufallsgehalt als jede der beiden Eingangssignale aufweist, d.g. das Ausgangssignal ist zufälliger als jedes der Eingangssignale.

In Fig. 5 ist ein weiteres Ausführungsbeispiel eines Zufallssignal- bzw. Zufallszahlengenerators 1 gezeigt, dessen Aufbau im wesentlichen demjenigen nach Fig. 3 entspricht, jedoch mit dem Unterschied, daß der zweite Eingang 8a, 8b, 8c jedes der Exklusiv-Oder-Gatter 4a, 4b, 4c jeweils mit dem Datenausgang 9c, 9a, 9b eines Speicherelements 5c, 5a, 5b einer anderen Funktionsgruppe 2b, 2c, 2a verbunden ist.

Bei den Ausführungsbeispielen nach Fig. 3 und 5 weist der Zufallssignalgenerator jeweils einen parallelen Zufallssignalausgang auf. Dieser hat mehrere Anschlüsse, die jeweils mit einem Datenausgang 9a, 9b, 9c, 9d eines Speicherelements 5a, 5b, 5c, 5d oder eines Zwischenspreicherelements 12 verbunden sind. Bei den Ausführungsbeispielen nach Fig. 4 und 6 ist jeweils ein serieller Zufallssignalausgang vorgesehen, der mit dem Ausgang des Zwischenspreicherelements 12 verbunden ist.

Wie aus Fig. 7 erkennbar ist, weisen die einzelnen Zufallsfolgengeneratoren 3a, 3b, 3c jeweils einen spannungsgesteuerten Oszillator 14a, 14b, 14c auf, der einen Frequenzsteuereingang 15a, 15b, 15c hat, der mit dem Ausgang einer Rauschspannungsquelle 16a, 16b, 16c verbunden ist. Der Oszillatorausgang jeder der Oszillatoren 14a, 14b, 14c ist jeweils mit dem Eingang eines Flip-Flop 17a, 17b, 17c verbunden, dessen Ausgang den Zufallsfolgensignalausgang 7a, 7b, 7c bildet. Zum Zurücksetzen des an dem Zufallsfolgensignalausgang 7a, 7b, 7c anliegenden Zufallsfolgensignal haben die Flip-Flops 17a, 17b, 17c jeweils einen

Rücksetzeingang. Die Rücksetzeingänge sind mittels einer Rücksetzleitung 18 untereinander und mit einem Mikroprozessor 19 verbunden. In dem Mikroprozessor 19 sind die Exklusiv-Oder-Gatter 4a, 4b, 4c, die Speicherelemente 5a, 5b, 5c und die Zwischenspeicherelemente 12 angeordnet.

Erwähnt werden soll noch, daß die die Zufallsfolgengeneratoren 3a, 3b und/oder 3c bei den Ausführungsbeispielen nach Fig. 3 bis 6 auch gemäß Fig.1 ausgebildet sein können und wenigstens zwei nichtdeterministische Zufallsfolgengeneratoren (30a, 30b) und zumindest ein Exklusiv-Oder-Gatter (40a) aufweisen können.

Patentansprüche

1. Verfahren zur Erzeugung eines Zufallssignals, wobei mittels wenigstens zweier nichtdeterministischer Zufallsfolgengeneratoren (30a, 30b) zumindest zwei Zufallsfolgensignale erzeugt und exklusiv-oder-verknüpft werden und wobei das Exklusiv-Oder-Ausgangssignal das Zufallssignal oder ein Zwischensignal zur Weiterverarbeitung bildet.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Exklusiv-Oder-Ausgangssignal als Zwischensignal mit dem Zufallsfolgensignal wenigstens eines weiteren nichtdeterministischen Zufallsfolgengenerators (30c) exklusiv-oder-verknüpft wird und das Exklusiv-Oder-Ausgangssignal dieser Verknüpfung das Zufallssignal oder ein Zwischensignal zur Weiterverarbeitung bildet.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß aus dem Zwischensignal ein Zufallssignalwert ermittelt wird, indem einem Exklusiv-Oder-Glied (40c) dieses Zwischensignals sowie ein zwischengespeichertes Ausgangssignal des Exklusiv-Oder-Gliedes (40c) zugeführt wird.

4. Verfahren zur Erzeugung eines Zufallssignals, wobei mittels wenigstens zweier nichtdeterministischer Zufallsfolgengeneratoren (3a, 3b, 3c) wenigstens zwei Zufallsfolgensignale erzeugt werden,

 a) wobei jeweils ein Zufallssignalwert aus jedem der Zufallsfolgensignale der einzelnen Zufallsfolgengeneratoren (3a, 3b, 3c) ermittelt wird und mit einem einem anderen Zufallsfolgengenerator (3b, 3c, 3d) zugeordneten Speicherwert exklusiv-oder-verknüpft wird,

 b) wobei das Ergebnis dieser Verknüpfung jeweils als neuer, dem zuerstgenannten Zufallsfolgengenerator (3a, 3b, 3c)

zugeordneten Speicherwert zwischengespeichert wird,

c) wobei die Verfahrensschritte a) und b) als Schleife wenigstens einmal erneut durchlaufen werden

d) und wobei danach die den einzelnen Zufallsfolgengeneratoren (3a, 3b, 3c) jeweils zugeordneten Speicherwerte als Zufallssignal ausgegeben werden.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Verfahrensschritte a) bis d) mehrmals durchlaufen werden.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß die Speicherwerte in einem Datenspeicher zyklisch verschoben werden.

7. Verfahren nach einem der Ansprüche 4 bis 6, dadurch gekennzeichnet, daß die Zufallsfolgengeneratoren (3a, 3b, 3c) jeweils vor dem erneuten Abarbeiten des Verfahrensschritts a) in einen definierten Zustand zurückgesetzt werden.

8. Verfahren nach einem der Ansprüche 4 bis 7, dadurch gekennzeichnet, daß die Verfahrensschritte a) bis d) mittels eines Mikroprozessors ausgeführt werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß zum Erzeugen der Zufallsfolgensignale der Zufallsfolgengeneratoren (3a, 3b, 3c) jeweils die Frequenz eines spannungsgesteuerten Oszillators (14a, 14b, 14c) mittels eines Rauschspannungssignals verändert wird und daß der Zufallssignalwert jeweils aus dem Oszillatorsignal des Oszillators (14a, 14b, 14c) ermittelt wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß jeweils vor dem erneuten Abarbeiten des

Verfahrensschritts a) eine definierte Zeitdauer, die gleich oder größer als die Periodendauer des Oszillatorsignals ist, abgewartet wird.

11. Zufallssignalgenerator (10), mit wenigstens zwei nicht-deterministischen Zufallsfolgengeneratoren (30a, 30b) und mit zumindest einem Exklusiv-Oder-Gatter (40a), wobei die Eingänge des Exklusiv-Oder-Gatters (40a) mit Zufallsfolgensignale liefernden Zufallsfolgengeneratoren (30a, 30b) verbunden sind, und wobei der Ausgang (100a) des Exklusiv-Oder-Gatters (40a) direkt oder indirekt über eine Zwischenstufe zur Weiterverarbeitung des Exklusiv-Oder-Gatter-Ausgangssignales mit einem Zufallssignal-Ausgang (90) des Zufallssignalgenerators (1) verbunden ist.

12. Zufallssignalgenerator (1) nach Anspruch 11, dadurch gekennzeichnet, daß die Zwischenstufe ein Exklusiv-Oder-Gatter (40b) aufweist, dessen einer Eingang (60b) mit dem Ausgang (100a) des mit den Zufallsfolgengeneratoren (30a, 30b) verbundenen Exklusiv-Oder-Gatter (40a) und dessen anderer Eingang (80b) mit dem Zufallsfolgensignal-Ausgang (70c) eines weiteren Zufallsfolgengenerators (30c) verbunden ist, und daß der Ausgang (100b) dieses Exklusiv-Oder-Gatters (40b) direkt oder indirekt über eine Zwischenstufe zur WeiterverarbeitungdesExklusiv-Oder-Gatter-Ausgangssignales mit dem Zufallssignal-Ausgang (90) des Zufallssignalgenerators (1) verbunden ist.

13. Zufallssignalgenerator (1) nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß die Zwischenstufe ein Exklusiv-Oder-Gatter (40c) aufweist, dessen einer Eingang (60c) direkt oder indirekt über eine weitere Zwischenstufe mit dem Ausgang (100a) des mit den Zufallsfolgengeneratoren (30a, 30b) verbundenen Exklusiv-Oder-Gatter (40a) verbunden ist, und

daß an den Ausgang des zuerstgenannten Exklusiv-Oder-Gatters (40c) ein Speicherelement (50) angeschlossen ist, dessen Ausgang über eine Rückkoppelschleife mit dem zweiten Eingang (80c) dieses Exklusiv-Oder-Gatters (40c) verbunden ist.

14. Zufallssignalgenerator (1), wobei der Zufallssignalgenerator (1) wenigstens zwei Funktionsgruppen (2a, 2b, 2c) hat, die jeweils einen nichtdeterministischen Zufallsfolgengenerator (3a, 3b, 3c), ein Exklusiv-Oder-Gatter (4a, 4b, 4c) und ein Speicherelement (5a, 5b, 5c) aufweisen, wobei das Exklusiv-Oder-Gatter (4a, 4b, 4c) jeder Funktionsgruppe (2a, 2b, 2c) jeweils mit einem seiner beiden Eingänge (6a, 6b, 6c) mit einem Zufallsfolgensignal-Ausgang (7a, 7b, 7c) des Zufallsfolgengenerators (3a, 3b, 3c) der Funktionsgruppe (2a, 2b, 2c) und mit seinem anderen Eingang (8a, 8b, 8c) mit einem Datenausgang (9a, 9b, 9c) des Speicherelements (5a, 5b, 5c) der Funktionsgruppe (2a, 2b, 2c) verbunden ist, wobei der Ausgang (10a, 10b, 10c) des Exklusiv-Oder-Gatters (4a, 4b, 4c) jeder Funktionsgruppe (2a, 2b, 2c) jeweils mit dem Dateneingang (11a, 11b, 11c) des Speicherelements (5a, 5b, 5c) der Funktionsgruppe (2a, 2b, 2c) verbunden ist, und wobei die Speicherelemente (5a, 5b, 5c) der Funktionsgruppen (2a, 2b, 2c) zum Verschieben ihrer Speicherinhalte über Datenleitungen (13) miteinander verbunden sind.

15. Zufallssignalgenerator (1), wobei der Zufallssignalgenerator (1) wenigstens zwei Funktionsgruppen (2a, 2b, 2c) hat, die jeweils einen nichtdeterministischen Zufallsfolgengenerator (3a, 3b, 3c), ein Exklusiv-Oder-Gatter (4a, 4b, 4c) und ein Speicherelement (5a, 5b, 5c) aufweisen, wobei das Exklusiv-Oder-Gatter (4a, 4b, 4c) jeder Funktionsgruppe (2a, 2b, 2c) jeweils mit einem seiner beiden Eingänge (6a, 6b, 6c) mit einem Zufallsfolgensignal-Ausgang (7a, 7b, 7c) des Zufallsfolgengenerators (3a, 3b, 3c) der Funktionsgruppe

(2a, 2b, 2c) und mit seinem anderen Eingang (8a, 8b, 8c) mit einem Datenausgang (9c, 9a, 9b) des Speicherelements (5c, 5a, 5b) einer anderen Funktionsgruppe (2b, 2c, 2a) verbunden ist, und wobei der Ausgang (10a, 10b, 10c) des Exklusiv-Oder-Gatters (4a, 4b, 4c) jeweils mit dem Dateneingang (11a, 11b, 11c) des Speicherelements (5a, 5b, 5c) der zuerst genannten Funktionsgruppe (2a, 2b, 2c) verbunden ist.

16. Zufallssignalgenerator (1) nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, daß das Speicherelement (5a, 5b, 5c, 50) oder die Speicherelemente (5a, 5b, 5c, 50) Teil eines Ringschieberegister sind.

17. Zufallssignalgenerator (1) nach einem der Ansprüche 14 bis 16, dadurch gekennzeichnet, daß das Ringschieberegister zusätzlich zu den Speicherelementen (5a, 5b, 5c) der Funktionsgruppen (2a, 2b, 2c) Zwischenspeicherelemente (12) aufweist.

18. Zufallssignalgenerator (1) nach einem der Ansprüche 11 bis 17, dadurch gekennzeichnet, daß die Zufallsfolgengeneratoren (3a, 3b, 3c, 30a, 30b, 30c) einen Rücksetzeingang aufweisen, mittels dem die Zufallsfolgensignale der Zufallsfolgengeneratoren (3a, 3b, 3c, 30a, 30b, 30c) in einen definierten Zustand überführbar sind.

19. Zufallssignalgenerator (1) nach einem der Ansprüche 11 bis 18, dadurch gekennzeichnet, daß die Zufallsfolgengeneratoren (3a, 3b, 3c, 30a, 30b, 30c) jeweils einen spannungsgesteuereten Oszillator (14a, 14b, 14c) aufweisen, dessen Frequenzsteuereingang (15a, 15b, 15c) mit einer Rauschspannungsquelle (16a, 16b, 16c) verbunden ist und daß der Oszillator-Ausgang mit dem Zufallsfolgensignalausgang (7a,

7b, 7c, 70a, 70b, 70c) des Zufallsfolgengenerators (3a, 3b, 3c, 30a, 30b, 30c) verbunden ist.

20. Zufallssignalgenerator (1) nach einem der Ansprüche 11 bis 19, dadurch gekennzeichnet, daß der Oszillator-Ausgang mit dem Eingang eines Flip-Flops (17a, 17b, 17c) oder dergleichen Frequenzteiler verbunden ist und daß der Ausgang des Flip-Flops (17a, 17b, 17c) mit dem Zufallsfolgensignalausgang (7a, 7b, 7c, 70a, 70b, 70c) des Zufallsfolgengenerators (3a, 3b, 3c, 30a, 30b, 30c) verbunden ist.

21. Zufallssignalgenerator (1) nach einem der Ansprüche 11 bis 21, dadurch gekennzeichnet, daß zumindest das oder die Exklusiv-Oder-Gatter (4a, 4b, 4c, 40a, 40b, 40c) und gegebenenfalls das Ringschieberegister Teil eines Mikroprozessors (19) sind.

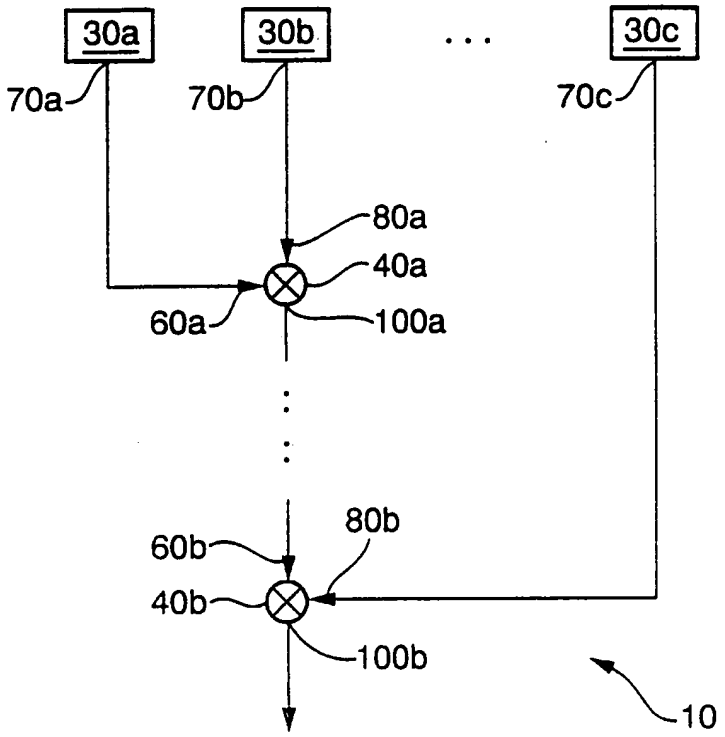


Fig. 1

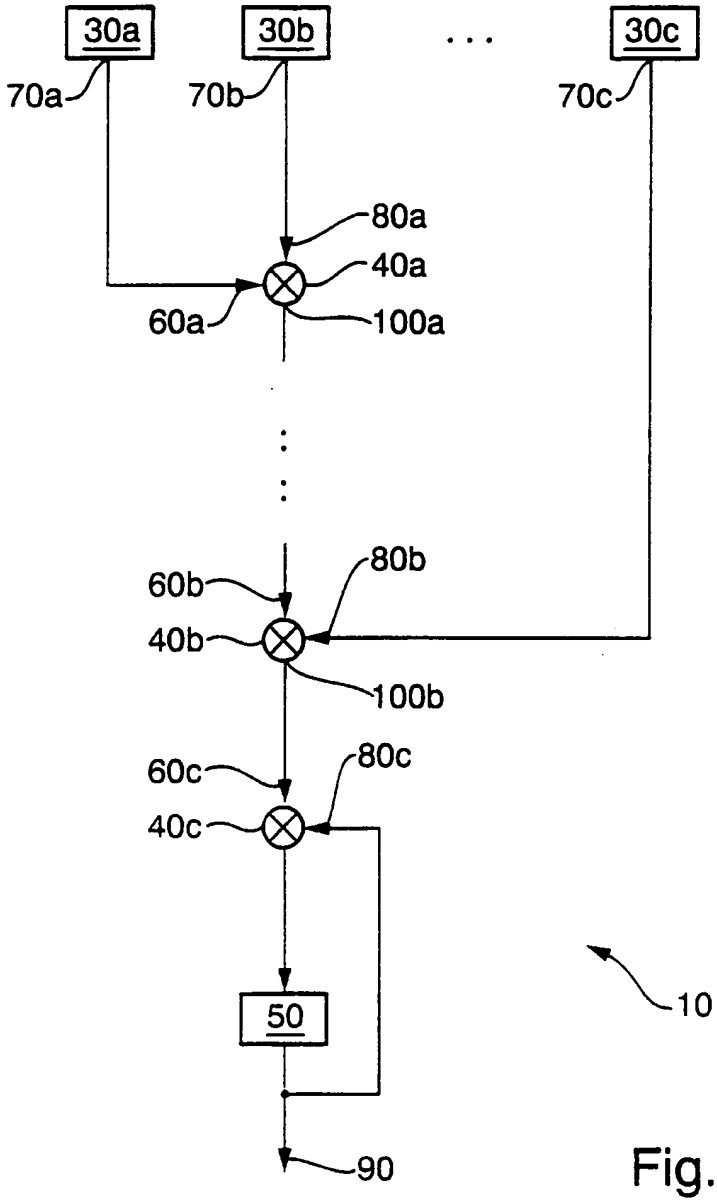

30a
30b
30c
70a
70b
70c
80a
40a
60a
100a
60b
80b
40b
100b
60c
80c
40c
50
10
90

Fig. 2

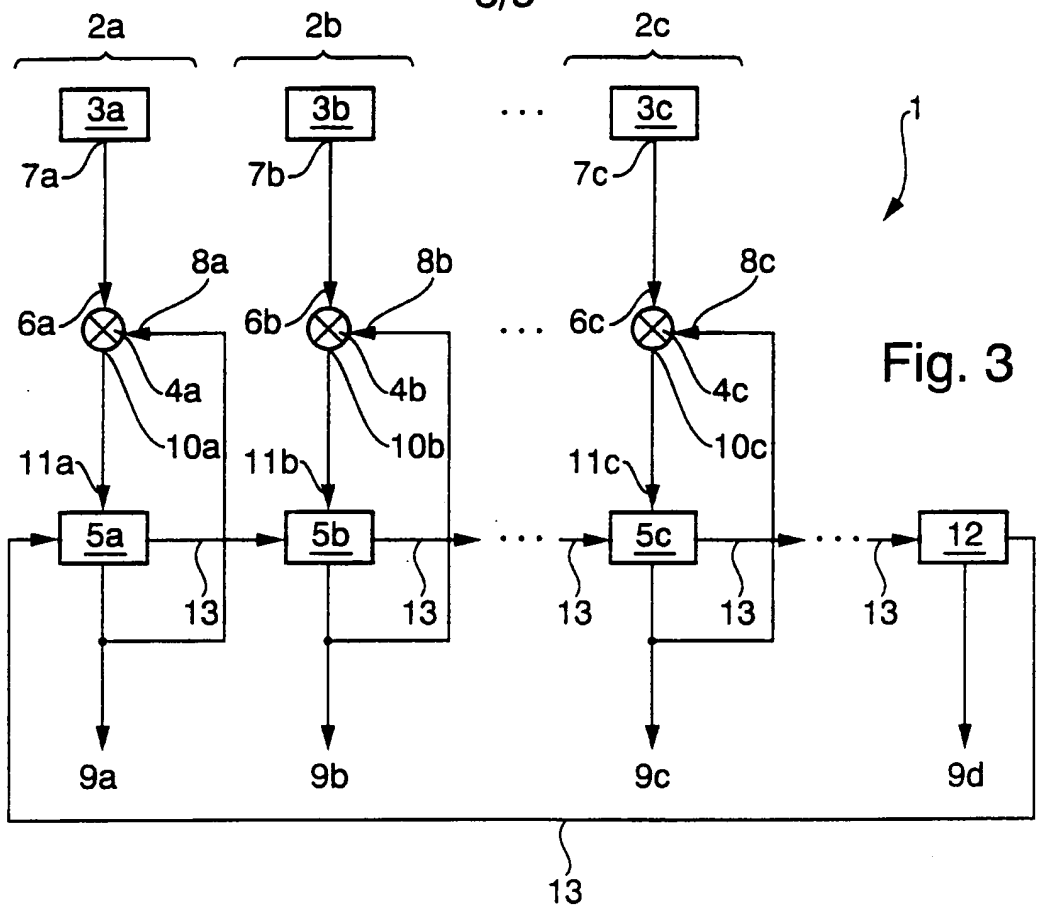

2a
2b
2c
3a
3b
3c
1
7a
7b
7c
8a
8b
8c
6a
6b
6c
4a
4b
4c
10a
10b
10c
11a
11b
11c
5a
5b
5c
12
13
9a
9b
9c
9d

Fig. 3

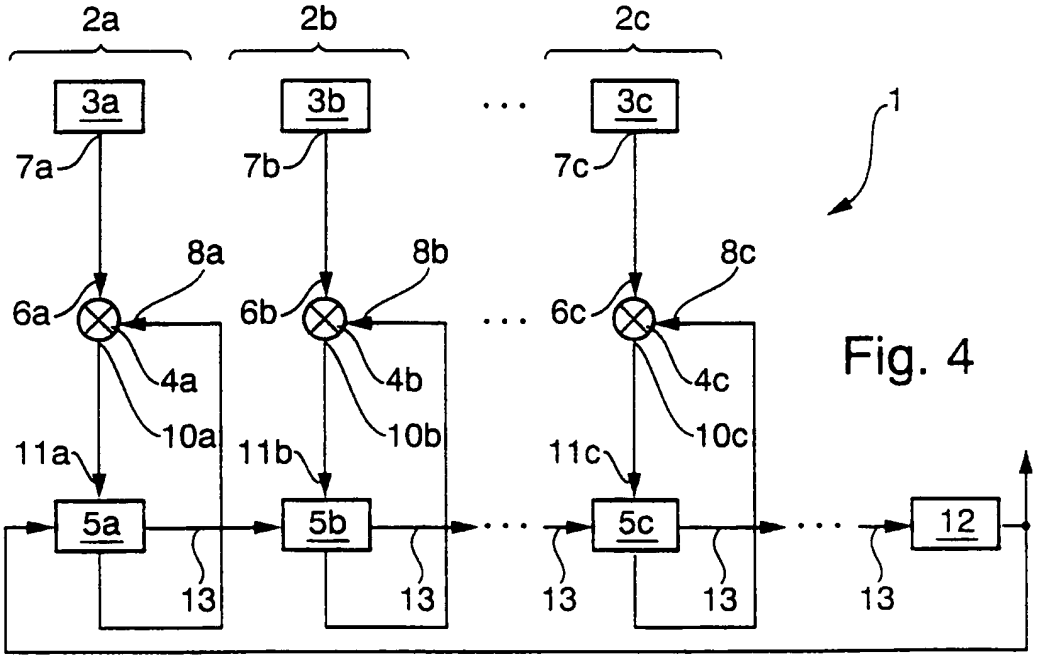

2a
2b
2c
3a
3b
3c
1
7a
7b
7c
8a
8b
8c
6a
6b
6c
4a
4b
4c
10a
10b
10c
11a
11b
11c
5a
5b
5c
12
13

Fig. 4

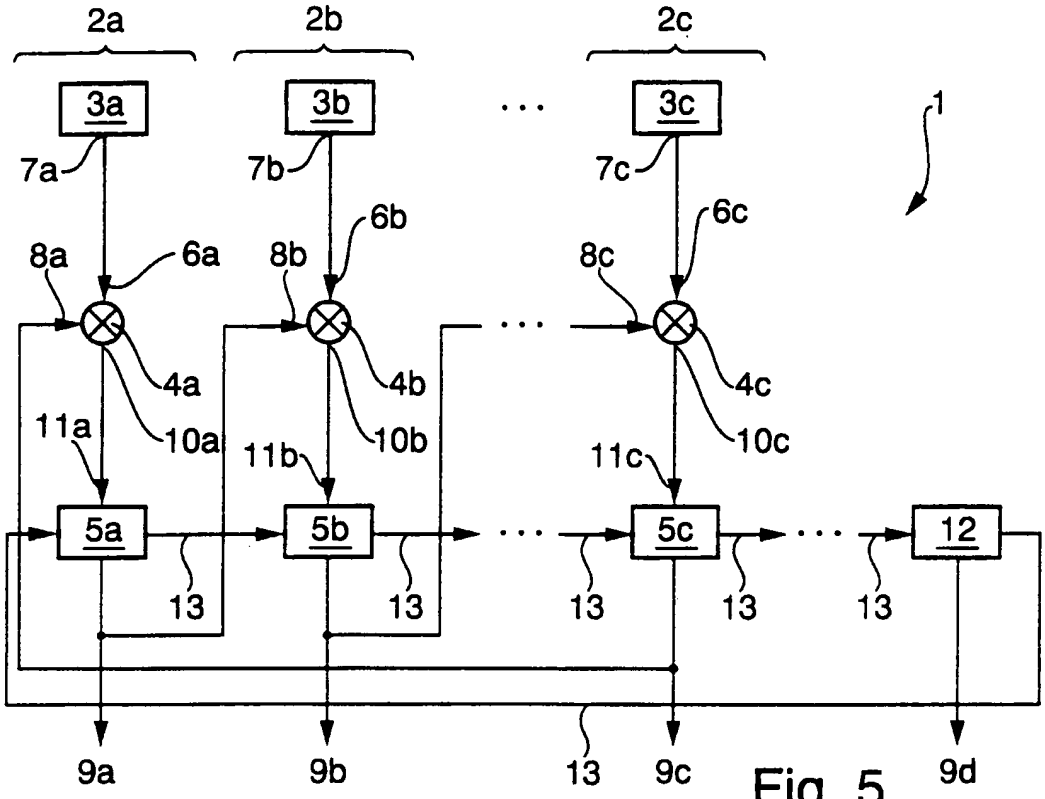

2a
2b
2c
3a
3b
3c
1
7a
7b
7c
6b
6c
8a
6a
8b
8c
4a
4b
4c
10a
10b
10c
11a
11b
11c
5a
5b
5c
12
13
9a
9b
9c
9d

Fig. 5

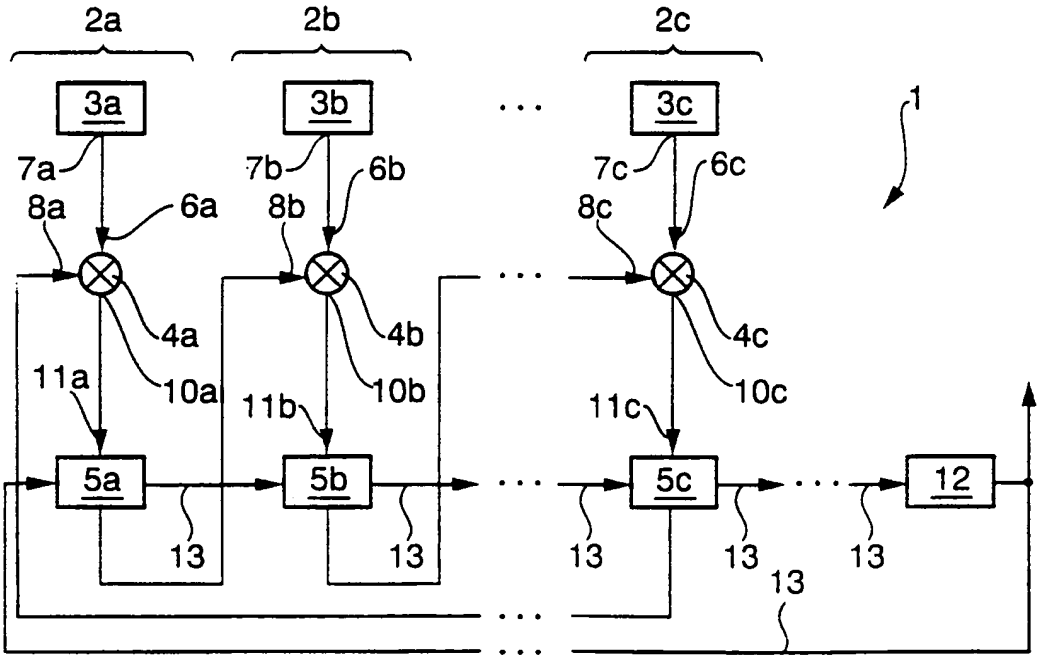

2a
2b
2c
3a
3b
3c
1
7a
7b
7c
6b
6c
8a
6a
8b
8c
4a
4b
4c
10a
10b
10c
11a
11b
11c
5a
5b
5c
12
13

Fig. 6

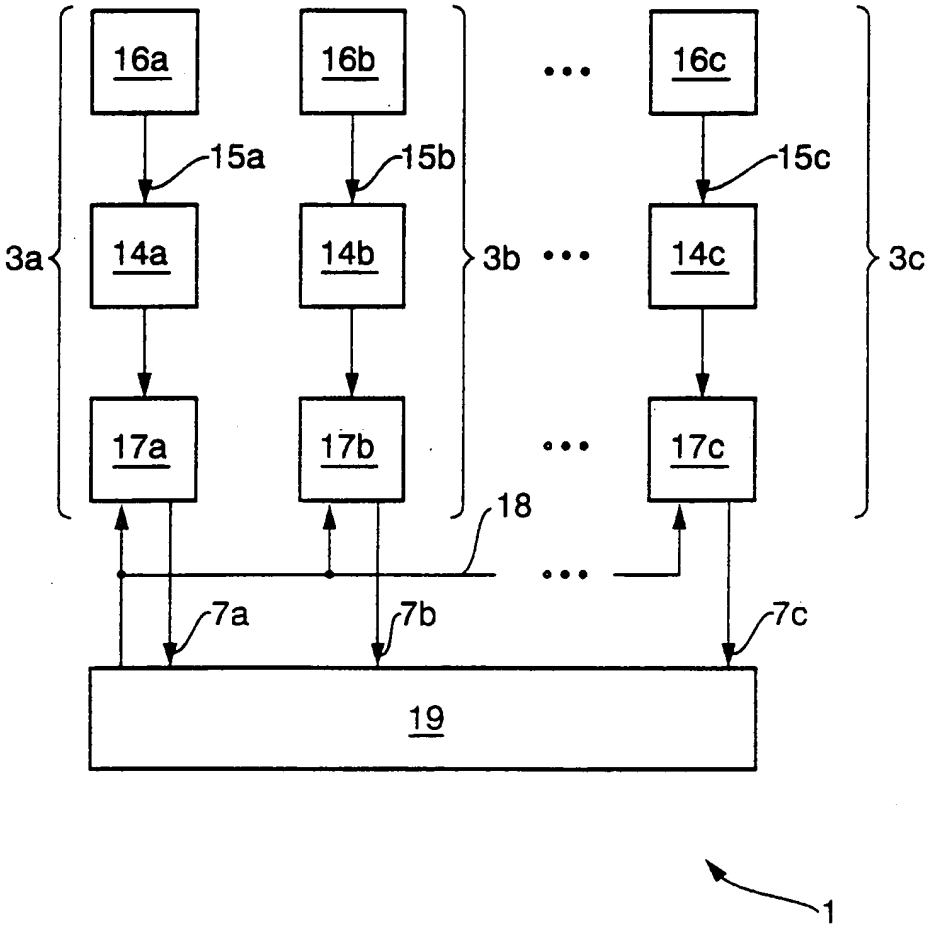

16a
16b
16c
15a
15b
15c
3a
14a
14b
3b
14c
3c
17a
17b
17c
18
7a
7b
7c
19
1

Fig. 7

INTERNATIONAL SEARCH REPORT

Internation. ...plication No
PCT/EP 00/01993

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H03K3/84

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H03K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Alpha-particle random number generator" IBM TECHNICAL DISCLOSURE BULLETIN., vol. 30, no. 9, February 1988 (1988-02), pages 337-339, XP002140868 IBM CORP. NEW YORK., US ISSN: 0018-8689 page 338, line 15 - line 38; figure 1	1,2,11, 12
Y	---	3-5,7,9, 13-15, 18,19
Y	EP 0 119 972 A (ERICSSON TELEFON AB L M) 26 September 1984 (1984-09-26) page 2, line 29 -page 3, column 14; figure 2	3,13
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 June 2000	06/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cantarelli, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 00/01993

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 87 01836 A (THINKING MACHINES CORP) 26 March 1987 (1987-03-26) page 7 -page 16, line 7; figure 1 ---	4,5,7, 14,15,18
Y	PETRIE C S ET AL: "MODELING AND SIMULATION OF OSCILLATOR-BASED RANDOM NUMBER GENERATORS" IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS),US,NEW YORK, IEEE, 1996, pages 324-327, XP000704602 ISBN: 0-7803-3074-9 page 324, right-hand column, last paragraph -page 325, left-hand column, line 13; figure 2 -----	9,19

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internation pplication No
PCT/EP 00/01993

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0119972 A	26-09-1984	SE 435979 B	29-10-1984
		DE 3460414 D	11-09-1986
		SE 8301380 A	15-09-1984
WO 8701836 A	26-03-1987	US 4691291 A	01-09-1987
		AT 98387 T	15-12-1993
		CA 1260078 A	26-09-1989
		DE 3689377 D	20-01-1994
		DE 3689377 T	28-04-1994
		EP 0240546 A	14-10-1987
		JP 63501609 T	16-06-1988

INTERNATIONALER RECHERCHENBERICHT

Internation. Aktenzeichen
PCT/EP 00/01993

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H03K3/84

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H03K G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	"Alpha-particle random number generator" IBM TECHNICAL DISCLOSURE BULLETIN., Bd. 30, Nr. 9, Februar 1988 (1988-02), Seiten 337-339, XP002140868 IBM CORP. NEW YORK., US ISSN: 0018-8689 Seite 338, Zeile 15 - Zeile 38; Abbildung 1	1,2,11, 12
Y	---	3-5,7,9, 13-15, 18,19
Y	EP 0 119 972 A (ERICSSON TELEFON AB L M) 26. September 1984 (1984-09-26) Seite 2, Zeile 29 -Seite 3, Spalte 14; Abbildung 2	3,13
	--- -/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahellegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des Internationalen Recherchenberichts
23. Juni 2000	06/07/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cantarelli, R

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internation Aktenzeichen
PCT/EP 00/01993

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	WO 87 01836 A (THINKING MACHINES CORP) 26. März 1987 (1987-03-26) Seite 7 -Seite 16, Zeile 7; Abbildung 1 ---	4,5,7, 14,15,18
Y	PETRIE C S ET AL: "MODELING AND SIMULATION OF OSCILLATOR-BASED RANDOM NUMBER GENERATORS" IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS),US,NEW YORK, IEEE, 1996, Seiten 324-327, XP000704602 ISBN: 0-7803-3074-9 Seite 324, rechte Spalte, letzter Absatz -Seite 325, linke Spalte, Zeile 13; Abbildung 2 -----	9,19

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/01993

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0119972 A	26-09-1984	SE 435979 B	29-10-1984
		DE 3460414 D	11-09-1986
		SE 8301380 A	15-09-1984
WO 8701836 A	26-03-1987	US 4691291 A	01-09-1987
		AT 98387 T	15-12-1993
		CA 1260078 A	26-09-1989
		DE 3689377 D	20-01-1994
		DE 3689377 T	28-04-1994
		EP 0240546 A	14-10-1987
		JP 63501609 T	16-06-1988